FOIA, Privacy & Records Management Conference 2009

Office of the Administrative Assistant to the Secretary of the Army

Records Management and Declassification Agency

Privacy Program Overview
Basic Privacy Principles

Leroy Jones, Jr.
Army Privacy Office
(703) 428-6185
leroy.jonesjr1@us.army.mil

Margaret Hamrick
Army Privacy Office
(703) 428-6193
margaret.hamrick@us.army.mil

The Privacy Act of 1974

- Reasons for the Act:
  - Individuals were often denied access to records the government maintained on them – the Act balances the government's need to collect information with the Privacy rights of individuals
- Key Principles:
  - Grant individuals rights of access to records maintained on them
  - Allow individuals to seek amendment of their records
    - ✓ Inaccurate, irrelevant, untimely or incomplete
  - Provide a Privacy Act statement as information is collected
    - ✓ Authority, Purpose, Routine Uses, Voluntary or Mandatory
  - Publish record collections on individuals in the Federal Register
    - ✓ System of Record Notices
  - Restrict disclosure/sharing between government agencies
    - ✓ Publish Computer Matching Agreements in the Federal Register

Budget

November 2000 - Circular A-130 - Management of Federal Information Resources

- Defines schedule of reviews of Privacy Act requirements
  - Annually:
    - ✓ Computer Matching: ensure that statutory, regulatory and OMB guidelines have been met for each ongoing matching program
  - Biennially:
    - ✓ Section (m) Contracts: ensure the wording of random contracts for system of records binds the contractor to the Act
    - ✓ Recordkeeping Practices: assure compliance with the Act and maintenance of automated records, disposal policies/practices
    - ✓ Privacy Act Training: ensure that agency personnel are familiar with the requirements of the Act and implementing regulation
    - ✓ Violations: determine the extent and prevent recurrence of agency civilly liable or employee criminally liable findings
    - ✓ System of Record Notices: ensure accuracy of descriptions
  - Every Four Years:
    - ✓ Routine Use Disclosures: ensure recipient's use continues to be compatible with the purpose of the disclosing agency collection
    - ✓ Exemption of Systems of Records: determine whether exemption is still needed

2002

Federal Information Security Management Act

- Reasons for the Act:
  - Technology and automation throughout the government caused concerns about protection, use and disclosure of information maintained on individuals - protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to ensure integrity, confidentiality and availability of data
- Key Principles:
  - Agency funding for automation contingent upon assurances of security and authorized collection and use
  - Privacy Impact Assessments (PIAs)
    - ✓ Analysis of automated systems containing information on individuals
  - Annual and Quarterly Reporting
    - Statistics on a wide range of agency Privacy practices
    - Narrative descriptions and responses to directed questions

2006 – VA Loss of Laptop

- Resulted in unprecedented heightened interest in Privacy
  - Presidential, Congressional, media, public, leadership
- Numerous directives culminated latest guidance
  - May 07 - OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
  - June 09 - DoD Memorandum, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- Established PII Breach Reporting
  - Purpose is to alert the appropriate authorities and those affected when a loss, theft, or compromise of government PII occurs
  - 1 hour to U.S. Computer Emergency Readiness Team (US-CERT)
  - 24 hours to Army Privacy Office
  - 10 working days for activities to notify individuals if warranted
- Army and DoD Leadership are provided PII breach reports
- Occasional Congressional and Presidential involvement

Implementing Recommendations of the 9/11 Commission Act of 2007
Public Law 110-53, Section 803

- Purpose: Review development and implementation of laws, regulations, procedures, policies, and guidelines relating to protecting the Nation against terrorism to ensure they balance with the need to protect Privacy
- Appoint a senior officer to serve as the principal advisor to the department head and other officials in appropriately considering privacy concerns
  - DAASA appointed and serves as Army Senior Agency Official for Privacy
  - Army Privacy Office charged with implementation and oversight
- Key requirements:
  - Establish procedures to redress privacy violation complaints
  - Provide advice on governmental powers and privacy
  - Submit quarterly reports to Congress and Privacy Board
    - ✓ Number and types of reviews undertaken
    - ✓ Type of advise provided and response given
    - ✓ Number of complaints, description and disposition

Definition of PII

Personally Identifiable Information (PII)

- Is any information that can be used to distinguish or trace an individual's identity such as name, social security number (SSN), date of birth, home address, home phone number, personal email address, financial information, fingerprint, photograph, medical information, and civilian National Security Personnel System (NSPS) data.

- Or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Definition of PIA

Privacy Impact Assessment (PIA)

- Is an analysis of how information is handled:
- Conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- Determine the risks and effects of collecting, maintaining and disseminating information in identifiable electronic form;
- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Purpose of the PIA

To analyze how PII is handled in order to:

- Determine conformance with applicable legal, regulatory, and policy requirements regarding privacy
- Assess the risks and effects of collecting, maintaining and disseminating PII
- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

When is a PIA required?

- System that collect, maintain, use, or disseminate PII on the general public, federal personnel (government civilians, members of the military, and Non-appropriated fund employees), contractors, and Foreign Nationals employed on military bases overseas;
- Prior to developing or purchasing new DoD information or electronic systems, (this includes DoD information systems and electronic collections supported through contracts with external sources that collect, maintain, use, or disseminate PII);
- There is a significant change to a system, to include new application functionalities or changes in privacy risk;
- For legacy systems;
- When converting from paper-based records that contain PII to an electronic system.

PIA REQUIREMENTS OVERVIEW

- Must be submitted on New form – DD Form 2930
- PIAs must be reviewed and updated every three years in conjunction with the Certification and Accreditation (C&A) cycle as a component of the DoD Information Assurance Certification and Accreditation Process (DIACAP) package.
- A System of Records Notice (SORN), is required if a group of files (paper or electronic) are retrieved by name, date of birth, social security number, contains a personal identifier assigned to an individual.
- The authorities in the PIA and the SORN should be consistent (use this instead)

Key References

- Privacy Act of 1974, as amended, 5 U.S.C. § 552a
  http://www.justice.gov/opcl/privstat.htm

- FISMA
  https://www.rmda.army.mil/privacy/docs/FISMA-final.pdf

- 9/11 Commission Act
  http://www.nctc.gov/docs/ir-of-the-9-11-comm-act-of-2007.pdf

- Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft, 2 July 2008

- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, 22 May 2007
  http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf

Key References (con't)

- DoD DA&M Memorandum, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, 5 June 2009
  http://www.dodig.mil/fo/Privacy/policy.htm

- DoD CIO/G-6 Memorandum, Army Privacy Impact Assessment (PIA) Compliance, 31Jul 2009 (available)

- DoD Directive-Type Memorandum, DoD Social Security Number (SSN) Reduction Plan, 28 Mar 2008

http://www.dodig.mil/fo/Privacy/PDFs/pr080328ssn_28Mar08_DrChu.pdf

Questions???